



State of Iowa Enterprise Data Classification Security Standard

June 11, 2009

Purpose

This Standard establishes data classification requirements for state agencies with the goal of protecting the confidentiality, integrity and availability of state data.

Overview

The State of Iowa collects and manages vast quantities of information in both paper and electronic format. Some of the information collected and managed by agencies has special protections established by state and federal law. Agencies are responsible for safeguarding the information under their care.

Data classification provides a framework for managing information. By classifying information it is possible for agencies to make decisions about how the information should be protected during creation, storage, transfer, and disposal.

Scope

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Data Classification Standard are defined below:

- **Data Classification System:** A system/process for classifying information into categories based on the extent to which it must be protected.

Updates

This document will be reviewed at least every two years and updated as needed.

Enterprise Data Classification Standard

1. **Data Classification.** All data must be classified by the level of protection required. At a minimum data must be classified as either:
 - a. Confidential – Information protected by state or federal law, or
 - b. Public – Information not included in a protected classification.

Additional classifications may be used to meet agency requirements. For example, some organizations may use the category of:

- a. Sensitive: Not explicitly protected by law, but exposure could result in negative impact to government services, state government partners or citizens.
2. **Data Protection:** Agencies shall set protection requirements for each data classification level. Protections should consider different states of data (i.e. at rest, in transit and in use) and forms of data (electronic and paper).
3. **Reviews.** Agencies shall review their data classification system, and the information they collect, annually to ensure that the data classification levels remain valid.
4. **Assessment.** The ISO may assess agency compliance with this standard. Agencies will provide access to their classification standard and documentation on how specific data are classified. If violations of this standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).
5. **Notification:** On or before the effective date of this standard, agencies will provide the Chief Information Security Officer with a description of how they are classifying data and a description of the agency standard for protecting data in each classification type,

Effective Date This standard shall be effective September 1, 2009.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation.